AU/ACSC/JENNINGS/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Non-reputable Identity Management and Information Access Technologies for Improved Cyberspace Agility by 2035

by

Martin T. Jennings, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Roger Philipsek

Maxwell Air Force Base, Alabama

April 2010

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Illustrations

Abstract

The military's use of cyberspace as a warfighting domain in current operations is vulnerable to hackers and malware. Today's cyber defense strategy is based on trust and perimeter boundaries. This strategy provides the DoD with little room for strategic or tactical errors and exposes our information superiority advantages to unnecessary risk. Emerging threats are becoming more sophisticated and organized, eroding US asymmetric advantages in cyberspace. By 2035, the emerging threats posed by insiders, artificial intelligence, and nation-states such as China will require game-changing innovations to defend cyberspace. The goal of this research paper is to propose an identity management and information access solution capable of mitigating emerging threats to military cyberspace operations in the year 2035.

This solution requires overcoming eight major technical challenges. This paper answers the following question for DoD strategic planners: What technologies and programs should the DoD invest in today in order to mitigate emerging threats to freedom of action in cyberspace by 2035? It answers this question by surveying the existing operational environment and comparing it with three of the most probable emerging threats to cyber operations between now and 2035. Finally, the paper highlights a potential solution to these threats given current capabilities and uses backcasting to identify the required variables, policy changes, and technology challenges.

Chapter 1: Introduction

On 12 May 2008, the Deputy Secretary of Defense issued a memorandum formally defining cyberspace for the Department of Defense (DoD).[1] In this memo, Deputy Secretary Gordon England highlighted the importance of cyberspace in military operations. Specifically, he noted that combatant commands and other DoD components require "the ability to operate unhindered in cyberspace."[2] A related assessment published by the Office of the Secretary of Defense sheds light on some of the obstacles to attaining this requirement, stating that "networks are growing faster than we can defend them… unprotected networks surrender asymmetric advantage… attack sophistication is increasing… [and the] number of [network] events is increasing."[3]

The impact of this growth is amplified by the DoD's reliance on a perimeter-centric network security infrastructure, akin to the trench warfare strategies prevalent during WWI or the Maginot Line in WWII. Much like the introduction of disruptive innovations such as aerial reconnaissance, strategic bombing, and Blitzkrieg changed the face of land war in the last century; the DoD must develop game-changing innovations to counter an ever- increasing list of emerging threats to cyberspace operations in the future.

This paper highlights three emerging threats most likely to impact cyber operations by 2035: organized cyber attacks from nation-states such as China; the potential use of artificial intelligence as a hacker attack vector; and the anonymity enjoyed by nefarious insiders and external attackers who have breached the DoD's perimeter defenses.

Research Methodologies and Paper Organization

The research methods used in this paper are organized into three sections. The first section presents an overview of the current operational environment. In this section, environmental scanning techniques provide a synopsis of existing technologies, policies, and procedures that comprise cyberspace operations today. The second section highlights several emerging threats that have the potential to disrupt cyber operations by 2035. This second section uses environmental scanning combined with forecasting to convey the need for solutions to offset these threats.

The third section presents a potential solution to mitigate emerging threats discussed in the previous section. This third section leverages backcasting methodologies to walk the reader through a series of technology challenges and policy changes required to arrive at the proposed solution. This section is broken into eight key technology and policy challenges. This section also highlights anticipated timelines, required DoD policy changes, and areas where commercial research and development are needed. The proposed solution in this section will help lay a foundation for a program of planned investments and policy changes, thus answering the research question posed previously.

Chapter 2: Current Operational Environment

Lieutenant General Robert Elder, the former Commander of the 8th Air Force, reinforced the importance of cyber operations when he asserted, "the Air Force now recognizes that cyberspace ops is a potential center of gravity for the United States and, much like air and space superiority, cyberspace superiority is a prerequisite for effective operations in all warfighting domains."[4] Much like traditional warfighting domains, the cyber domain leverages protective fortifications such as firewalls and virtual private networks to dissuade an adversarial force and

protect friendly assets.[5] This fortification-centric security model, like the Maginot Line in WWII, is only effective if it is contiguous and unavoidable.[6] Attacking vectors only need to sidestep misconfigured defenses or find a small, unpatched hole to slip through in order to gain a foothold inside the perimeter. Once established, these attackers can operate unnoticed for some time as long as their actions do not trigger any alarms.

The DoD cyber infostructure of today is an infrastructure-dependant "trusted network." We see examples of this trust today in how users login to desktops. Once a user has access to the desktop, he or she is considered part of the trusted network, and all operations on that desktop are now trusted by the network regardless of whether the user changes or the session is hijacked by malware. This trust is especially worrisome on SIPRNET and higher classification networks where few controls exist beyond gaining initial access.

The methods used by the DoD to protect cyberspace today are not that far removed from the methods used to protect the first DoD networks in the 1990s. According to DISA's 2008 DoD NIPRNET Demilitarized Zone (DMZ) Engineering Plan, "The scope of the DoD DMZ effort is specifically to protect private DoD systems against attack from the Internet by establishing DoD DMZs and migrating Internet-facing DoD servers into DoD DMZs."[7] Deputy Secretary of Defense William J. Lynn III stated that "[a] fortress mentality will not work in cyber. Cyberwar is much more like maneuver warfare [where] new technologies [will] help us find and neutralize intrusions."[8] This capability requires the addition of several new core services that will provide identity infrastructures capable of finding and neutralizing threats.

Like the DoD's perimeter defense posture, core services offered to end users have changed little since the 1990s. In 1992, as the first base-level network control centers stood up out of necessity, the forerunners of today's cyber warriors identified groupings of standard core

services.[9] These core service groupings were centered initially around file sharing, electronic mail, printing, and name resolution for accessing remote computer addresses. In the late 1990s, as malware was starting to take its toll on the services provided to end users, virus protection and firewall boundaries were added. DISA's 2008 DoD DMZ Engineering Plan identified the addressed core services as "e-mail, domain name system (DNS) web, and file transfer protocol (FTP)."[10] The only things that have changed in the last 20 years are the scope of the user base serviced, the centralization of host servers, and reduction in administration personnel.

The DoD's current perimeter-centric security model targets primarily external threats and does little to monitor internal activity. This insider threat is further compounded by the DoD's lack of an enterprise-wide identity management capability to manage user access controls consistently.[11] A 2003 Gartner report highlights the four "A's" (authentication, authorization, auditing, and administration) needed to combat insider threats.[12] A core tenet of these new identity capabilities is non-repudiation. A non-reputable identity is undeniably valid and authentic; it cannot be falsified. The deployment of these identity capabilities will eliminate the anonymity found inside the DoD infostructure today.

The auditing and administration capabilities help identify abnormal patterns and perform rapid triage in the event of an attack.[13] Lieutenant General William T. Lord, Air Force Chief of Warfighting Information and Chief Information Officer, recently highlighted what he considered a "frightening" form of cyber attack.[14] He is worried about intentional manipulation of mission system data by insiders or external attackers[15] and that "incorrect decisions [will be made] based on information that has been changed."[16] Auditing and administration capabilities (discussed in Chapter 4) will help identify these changes regardless of whether the source is an insider or an intruder who slipped though the perimeter defenses.

Another method of limiting the internal data manipulation threat surface area is to institute controls on authorization. Gartner defines an identity management authorization capability as one that deals with controlling user access to content and applications based on security clearance and need-to-know.[17] Not every user requires access to an application or piece of information. Today's Internet-minded user seems fixated on expectations of access based on holding a security clearance commensurate with the classification of the network and little on need-to know or need-to-access at the file and system level.

Implementation of tiered access schemes centered on roles and entitlements will limit the amount of information accessible and modifiable by a given end user. The DoD has attempted to address the issue of authentication with the introduction of the Common Access Card (CAC). While more secure than passwords, the CAC is still vulnerable to unauthorized use. Attackers can steal CACs or socially engineer the pin associated with the CAC, and. most commonly, users may often walk away from an unlocked machine, leaving it at risk for exploitation. CACs also have several operational limitations. Users require secure access to classified information systems for the majority of their warfighting missions. Currently, CACs cannot be used to access classified networks, though plans for expansion to SIPRNET are underway. In reviewing the literature related to cyber operations, the author found identity management capabilities that are deployed at an enterprise level in the DoD today. Authentication is the most common focus of these identity management efforts, but planners often overlook auditing, administration, and authorization capabilities.

According to Lt Gen Lord, future communications "will use more advanced techniques to carry data on different waveforms."[18] These future capabilities will provide users with needed "secure connections and verifiable authenticity of data." [19] These future cyber needs must be

delivered through planned execution, resourcing, and development of technical capabilities designed to defend our cyber dominance in the face of asymmetric attacks and emerging threats.

Chapter 3: Emerging Threats

According to General Tom Hobbins, the former COMUSAFE and Air Force Chief Information Officer, the average time to prosecute a target dropped from 76 minutes during Operation DESERT STORM to as little as eight minutes in Operation IRAQI FREEDOM.[20] General Hobbins attributed this drastic drop in the kill chain during that 18- year period to the introduction of and increased reliance on communications and information- sharing capabilities.[21] He warned that this increase in capability had a trade-off in the form of increased dependence on cyberspace.[22] Because of this, the AF and the DoD are now more vulnerable to anything that threatens to disrupt cyberspace operations.[23] Three of the most serious threats to the DoD's cyber infrastructure are China, trends in artificial intelligence (AI), and the "nefarious" insider.

The National Defense Council stated in its Global Trends 2025 report that "the employment of new forms of warfare such as cyber and space warfare are providing state militaries and nonstate groups the means to escalate and expand future conflicts beyond the traditional battlefield."[24] Adversaries of the United States recognize the importance of information superiority and the DoD's dependence on its critical information infrastructure.[25] Because of the DoD's dependence, nation-states such as China, as well as non-state actors, have demonstrated and continue to invest in cyber attack capabilities.[26]

According to Brian Mazanac, in his article *The Art of (Cyber) War, "*[China] is increasingly developing and fielding advanced capabilities in cyberspace…capable of causing economic harm, damaging critical infrastructure, and influencing the outcome of conventional

armed conflicts."[27] China's cyber aspirations have been a core national strategy since 1990. China has invested in cyber exploitation, growing its espionage capabilities over the past two decades. China also is developing network attack capabilities in an attempt to strategically deter the United States from involvement in issues pertaining to Taiwan's independence.[28]

In a recent report to the US-China Economic and Security Review Commission, it was noted that "China will likely use its [cyber] capabilities to attack select nodes on the military's… NIPRNET and unclassified DoD and civilian contractor logistics networks" should a conflict erupt in the region.[29] Media reports of the "Titan Rain" espionage operation highlighted the ability of alleged state-sponsored Chinese hackers to successfully exploit DoD systems starting in 2003.[30] This is especially worrisome since the tools and skills required to mount a network attack in cyberspace are the same as those required to perform espionage.[31]

In addition to organized hacking activity by nation-states, the potential introduction of artificial intelligence (AI) poses a threat to the future of cyberspace operations. According to a recent article in *The Futurist*, "[I]nstead of relying on human hackers to carry out their attacks, antagonists will automate their information warfare, relying on AI systems to probe opposing defenses [and] carry out attacks."[32] The precursors to AI threats can already be seen in today's distributed denial of service attacks and bot-nets. Third-party machines are hijacked and used as remote agents for cyber attacks against military, political, economic, and information-centric targets in cyberspace.[33] These attacks become more sophisticated as processor power increases. According to Moore's Law, processing power historically doubles every twenty-four months.[34]

The threat of increasingly sophisticated automated attacks in cyberspace stands to overwhelm the DoD's ability to defend cyberspace. As AI enabled bot-nets and hacker tools become more self-directing, they will cause the DoD to take increasingly restrictive defensive

actions. Many of today's defensive actions involve limiting freedom of movement in cyberspace. This often restricts access for both the attacker and legitimate users. To better identify legitimate users, the DoD must eliminate anonymity within the protected confines of its perimeter defense system.

The existence of this anonymity inside the protective perimeter highlights another serious threat to the DoD's cyber capabilities, the insider threat. A non-reputable or trusted identity management capability consisting of the four "A"s discussed in Chapter 2 would eliminate stolen identities and limit the mobility of malware and nefarious insiders in cyberspace. As more sophisticated threats begin to emerge, the need for enterprise solutions to these issues will only increase.

Chapter 4: Proposed Solution

The year is 2035. Imagine that a series of increasingly more capable generations of wireless connectivity have transformed today's wireless networks. These networks have supplanted terrestrial broadband and DSL technologies and now provide high-speed cyber access from virtually every nation in the world. Combine land, sea, space, and airborne objective gateways with this civilian infrastructure, and the DoD has access to a nearly ubiquitous web of connectivity.

Moore's Law has continued to hold true for two more decades, providing users with handheld iPhone-like devices with processing power and storage rivaling the best desktop computers available today. A warfighter can now access all mission-critical applications and information from a single handheld device. This unified communications device is also a Global Positioning System receiver and a secure phone capable of dialing both commercial and military lines.

This device leverages the latest in wearable RFID authentication technology that provides multi-factor biometric verification.[35] This authentication information is passed through the handheld device to authentication and authorization servers for verification prior to granting access. Based on the warfighter's location and proximity to secure access points, he or she can also access classified information via the same device, provided he or she has the necessary authorization to do so.

The device maintains security level tagging on all information. This tagging prevents classified information access by unclassified applications. It also allows one-way unclassified information access to higher classification applications. Application-based and role-based access to information is presented during logon based on location, authorized access, and options selected. Data is mobile and stored independently of the application images. This allows data to persist and be shared between networks as classification rules allow.

A nation-state sponsored cyber antagonist launches a series of artificial intelligence augmented attacks against military targets in cyberspace. The attacker targets .mil network infrastructure, since it is easily discerned from the myriad of .com addresses. The attacks flood a series of routers and bring down access to a core server farm in Washington D.C. for several hours in an attempt to blind the Pentagon's information systems and disrupt strategic decision-making processes.

The unified communications devices are not affected because they are routing through the .com network and wireless broadband networks that are pervasive and difficult to disrupt. Military end users accessing information and applications housed in the Washington D.C. server farm are routed to other major nodes in the grid-computing infrastructure without missing a step. The computing load is shifted away from the now quarantined portion of the grid until the

affected systems can be reimaged and brought back online. The Pentagon populace is not affected by the attack. In fact, only a handful of people even know the attack took place.

To make this proposed solution a reality by 2035, a series of eight technical challenges must be overcome. To aid visualization, the eight challenges are also presented visually in Figure 1 in Appendix A. Please note that, for simplicity, the illustration only depicts four networks. In reality, the multitude of network classification caveats and combinations of caveats would necessitate a continuum of networks that cannot be accurately shown due to space constraints and the classification of this document.

The remainder of this chapter presents these challenges using the backcasting research methodology. This methodology highlights critical future steps and variables that must be overcome to make the potential solution a reality. If any of these steps fail to come to fruition, the entire solution fails. The eight challenges are presented in order of complexity and estimated effort to implement. For example, the first challenge has the longest anticipated time to implement and requires the most effort to realize.

"President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter."[36] In May 2009, President Obama determined that the Comprehensive National Cybersecurity Initiative (CNCI) and its associated activities developed under President Bush should become key elements of a broader, updated U.S. strategy.[37] Several of the initiatives enumerated by President Obama are in line with the recommended solution defined below.

Tech Challenge #1: Wearable RFID/Biometric Device Development

One of President Obama's cybersecurity strategy initiatives is to define and develop enduring "leap-ahead" technology, strategies, and programs.[38] "This initiative seeks to develop strategies and programs to enhance the component of the government R&D portfolio that pursues high-risk/high-payoff solutions to critical cybersecurity problems."[39] Tech Challenge 1 fits in this category. This tech challenge involves the creation of a wearable RFID device that presents a unique biometrically derived signature when interrogated. This device could be based on technologies such as Precision Dynamics Corporation's Smart Rewearable Wristband[40] (see Figure 2 in Appendix A). This watch- size device provides a unique RFID identity when interrogated.

This RFID technology, though available today, will require significant hardening and integration to become the solution required for military needs in 2035. First, the RFID signal will require encryption and must be muted such that it only responds to specific encrypted interrogation signals. This encryption and signal obfuscation is required to eliminate the potential for falsifying or hijacking of the RFID data. The RFID payload will be a unique identifier associated with the user that will only be transmitted if interrogated by a registered military device and the RFID transmitter is worn by the paired user.

This pairing highlights the second significant enhancement required to meet military needs by 2035. The RFID device must be integrated with several biometric sensors. These sensors, when used in combination, will provide multifactor biometric identity verification to the interrogating device. Biometrics operates on the principle of comparing a stored template (a digitized sample taken during the enrollment process) and a new sample taken at the time of

access. Current biometric options include fingerprints, iris scans, hand geometry, voice recognition, skin patterns, and facial recognition.[41]

While many of these biometric authentication methods are in use by the military today, next- generation biometric identifiers will be required to enable the passive nature and user experience desired for the proposed solution. These identifiers include neural wave analysis, skin luminescence, remote iris scan, advanced facial recognition, and body odor.[42] In 2008, Microsoft sought a patent for a system that would wirelessly monitor employees' unique biometric signatures. The application specifically calls out galvanic skin response, electromyography, and brain signals as well as several other biofeedback related indicators.[43] The combination of these indicators into a multimodal identification system meets the needs of the proposed solution.

The use of biometrics in a wireless environment requires security and encryption. Private biometric templating is a method of providing encrypted pseudo identity templates for comparison.[44] The use of these encrypted templates ensures that no unencrypted source identity representations are passed wirelessly or stored in a central location. An illustration of this enrollment and comparison process can be found in Figure 3 in Appendix A. This method of comparison is similar to the methods used to store and validate secure passwords on computer systems today.

This system must eliminate the possibility of false positives through the use of passive and active biometric and interactive challenge mechanisms. To this end, the final solution is envisioned to incorporate random biometric user challenges such as fingerprint scans, iris recognition, or PIN requirements based on the classification and location of the target device to

be accessed. The solution is also envisioned to be able to verify the end user is alive in order to eliminate post-mortem access.

Unfortunately, while these biometric sensors will be able to eliminate post-mortem access, they will not be able to eliminate coercion or duress situations. Duress and lockout PINs can be implemented in an attempt to counter this threat, but there is no foolproof method for eliminating this threat completely. If a user is complacent with the coercing agent, there is no method of preventing access based on the authentication portion of identity management alone. However, the threat can be mitigated through the integration of auditing and authorization identity management controls discussed later in this chapter.

This challenge is purely technical, but it relies heavily on commercial innovation and materials development variables to come to reality. As discussed earlier, some of the components required to meet this challenge are mature today. The development, miniaturization, and research required to integrate these technologies is well within the reach of the 2035 timeline. Due to the cost of R&D, there is most likely a limited market in the business world for this level of identity assurance. To meet the 2035 timeline, the DoD must begin programming for research initiatives and integration concepts today. Building on successful passive RFID-identity initiatives such as the Department of Homeland Security's Western Hemisphere Travel Initiative[45] would be an excellent point of departure.

Protecting biometric information is not necessary only to prevent unauthorized access. The nature of biometric data also impinges on the end user's privacy. Adjustments to policy are necessary to address two main issues with respect to biometric data: "information of the body" and "function creep". "Information of the body" deals with the concern over digitalization of a person's physical and behavioral attributes and their distribution across a global information

network.[46] Administrators must be able to handle this information in accordance with applicable privacy and medical information handling instructions.

”Function creep” is the term used to describe the expansion of a process or system, where data collected for one specific purpose is subsequently used for another unintended or unauthorized purpose.[47] This often happens without the knowledge of the end user. A prime example of function creep is a Social Security Number (SSN). The SSN is a primary identifier for many systems, and it now has purposes well beyond those originally intended. Biometric information and the inevitable “function creep” associated with it must be handled in a manner similar to SSNs. Notification and usage guidelines must be developed and ethical concerns addressed.

The ultimate goal is a set of wearable sensors that in combination provide a set of crucial passive biometric components to a non-reputable identity system. Realization of this biometric component and its associated RFID transmission capability requires government- funded commercial development and integration as well as significant policy changes over the course of the coming decades.

Tech Challenge #2: Unified Communications Device

The wearable device detailed in Tech Challenge 1 works in conjunction with unified communications devices to provide the authentication and end user access portions of the overall proposed solution. Tech Challenge 2 entails the creation of a series of dockable unified communications devices that are encrypted, remotely wipeable, and capable of running full applications as do desktop computers today.

These all-in-one handheld devices will be capable of accessing voice, video, web, and GPS data. Additionally, these devices can operate at multiple security levels, providing the end

user access to classified information in appropriate situations. The end solution is envisioned to be similar in form factor to an Apple iPad[48] or iPhone with the added functions of the Sectéra Edge Smartphone[49] and General Dynamics' TVE desktop.[50]

The device will have a multi- touch screen and virtual keyboard just like Apple's current iProducts. Motion sensors and GPS location capabilities provide contextual cuing based on movement through an environment, as well as navigational aids in unfamiliar locales. The device provides for biometric data capture such as fingerprint or facial recognition in support of random multifactor biometric challenges detailed under Tech Challenge 1. Additionally, the device has the capability to validate the end user through interrogation of the wearable RFID/biometric device detailed under Tech Challenge 1.

Much like the iPhone of today, this unified communications device (UCD) will be capable of accessing multiple networks for voice and data communications. In addition to accessing, Wi-Fi and cellular carriers worldwide, the UCD can access Wide Area Network protocols such as mobile Wi-Max (802.16m) and follow-on cellular data networks based on today's 3G and 4G technologies. These commercially hosted networks will provide the backbone for the majority of unclassified access worldwide, as depicted in Figure 1 in Appendix A. Individual devices will also be able to use each other to create ad-hoc peer-to-peer networks that will extend the reach of communications in obstructed and bandwidth- constrained environments.

Additionally, the UCD will include capabilities found in today's Sectéra Edge Smartphone. These will include the ability to access top secret, secret and unclassified voice and data networks via military gateways and hotspots. UCDs will be centrally managed and can be disabled and wiped if lost or stolen. Mobile user profiles, session state, and data will be centrally

stored. This will allow a user to move from any given station or device to another and pick up where he or she left off on the previous device.

The integration of multi-level networking capabilities like those found in General Dynamics' TVE desktop will allow access to different levels of classification simultaneously.[51] The multi-level networking capability will also allow data to be moved from lower to higher classifications. This desktop capability leverages virtual machine technology and will greatly enhance end user data sharing in coalition environments. The virtual machines are centrally housed, managed, and patched, eliminating the need for management of the end user devices. The use of centralized virtual machines will be discussed further in Tech Challenge 7.

The UCD will be dockable and a full replacement for today's desktop computers. Given Moore's Law, the processing and storage power of a device the size of an iPhone will dwarf that of today's high- end desktops by 2035. The UCD will also have an offline capability that will allow users to store and process information in bandwidth- constrained environments. This offline capability will allow for encrypted storage of unclassified data to protect it at rest.

Much like Tech Challenge 1, this challenge is mostly technical and relies heavily on commercial innovation and materials development variables. NSA certification will be required to enable mobile access to classified networks. Given the current NSA certifications and availability of the necessary building block technologies, an integrated and much more capable device will surely be available by 2035.

Tech Challenge #3: Bi-directional Guards and Meta Tagging

Tech Challenge 3 is the creation of bi-directional guard devices that allow the free flow of information from lower classification to higher classification networks as well as limited transfer from higher to lower. This challenge also deals with meta tagging of information for

proper handling by automated guard devices and coalition filters. As mentioned in the previous section, the TVE desktop environment provides unidirectional transfer of information. This free flow of information from lower to higher classification meets the requirements for part of this challenge.

The other direction can be handled by a system similar to the Multi Role Boundary Control (MRBC) – Information Support Server Environment (ISSE) System. This system integrates three guarding technologies to provide a comprehensive solution for the secure exchange of network management data, chat, instant messaging (IM), electronic mail (including attachments), and commonly used text and imagery file formats.[52] This system relies on a human review after the guard preprocesses and highlights potential issues.

Unfortunately, the human element will require the greatest changes. Technology aside, the larger issue becomes proper meta tagging of information, classification markings, and the sheer volume of information and data. In order to support automation and rapid movement of information from one network to another, significant information and knowledge management changes must take place.

The Multi National Force-Iraq (MNF-I) Concept of Operations for Knowledge Management highlights this need:

> A case for knowledge operations is based on the need to share, fuse, and present relevant information in the right format, and within the right decision cycle period, to yield decision superiority. We must shift our collective focus from information management to what we do with the information and how we properly direct its discovery, transmission, fusion, storage, and targeted use.[53]

Policy challenges required to implement knowledge and information management architectures are not the focus of this paper. However, it is important to note that knowledge and information

management overlap with identity management in several areas and may impact successful realization of several challenges described in this section.

As an example of this interrelationship, Figure 4 in Appendix A shows an example systems architecture that successfully supports information discovery, management, and archiving. Notice the reliance on identity management annotated on the right-hand edge of the block diagram. Identity management is pervasive across the entire system stack and is integral to successful implementation of the illustrated systems.

Figure 5 in Appendix A details the application- level support these MNF-I systems provide to the MNF-I staff processes and Lines of Operation. Again, identity management is illustrated as a key component supporting the applications delivered to the MNF-I staff. Using examples of successful information and knowledge management efforts such as these as a basis, the DoD enterprise solution for identity management as detailed in these challenges can be formulated and matured by 2035.

Currently, the AF's Air Combat Command is implementing an information management and knowledge management program called Ignite ACC. This campaign is a follow-on exploration initiative based on the technologies used in Iraq. Initiatives such as Ignite ACC are important because they focus on the people, processes, and information involved and not just the technology. The AF has been struggling with information and knowledge management for over ten years under its Enterprise Information Management (EIM) program. EIM has failed to provide an enterprise solution during this time because it focuses too heavily on the technology piece and not the human factors involved in managing information and tagging it for proper disposition.

The technology exists to enable the required information processing and meta tagging today. However, meta tagging and related semantic web capabilities are immature and not uniformly implemented.[54] This immaturity, combined with the workload and investment in human resources required to clean up the digital landfills that plague DoD's networks today, prevents agile flow of information between coalition partners and classification levels.[55] Carefully crafted policy and direction for meta tagging, information management, and implementation of guard devices is required to meet the 2035 deadline. Further, consolidation of all Service- and unit- level information management, knowledge management, and records management programs under the DoD Assistant Secretary of Defense Networks & Information Integration Office would reduce the amount of time and money spent on these policy- driven activities.

Tech Challenge #4: Ubiquitous Network Access

In a recent article in *The Economist*, Hamadoun Touré (Secretary-General of the International Telecommunications Union) stated that his organization expects mobile cellular teledensity to reach 100% worldwide by 2013.[56] He goes on to state that not only will every person in the world have access to cellular devices, but mobile broadband will become a global phenomenon by 2014.[57] He expects 3G and 4G subscribers to exceed 1.4 billion worldwide by that time.[58]

Leveraging an extrapolation of the widespread commercial infrastructure trends detailed above, the proposed solution would have access to voice and wireless broadband data networks nearly worldwide by 2035. The multi protocol- capable device seeks out the best connectivity available at any given time. If commercial networks are not available, the device may form ad-

hoc networks with authenticated devices in the vicinity. This ad-hoc bridge enables small group communications in austere locations and bridges core network dead spots.

Mobile military hotspots extend commercial and classified service into austere areas of operation. The proposed devices also have the ability to route over military networks when access points are in range. These military access points will enable access to unclassified as well as classified networks based on location and security of the environment. Location, availability of military access points, end user's need-to-access the associated classification level, and the end user's role drives the ability to access classified information. The concept of roles with respect to authorization and information access will be discussed under Tech Challenge 6.

This challenge also requires development of new methods of interconnecting .com, .mil, .smil, and caveated networks that mandate authentication at the packet level without impacting throughput. The required DoD level technologies and solutions fall under the DoD Cryptographic Modernization Initiative.

> The DoD Cryptographic Modernization Initiative will provide IA solutions to enable the Global Information Grid to securely employ its enterprise services, …weapons and communications systems, as well as interoperate with allies and coalition partners, activities that are essential to the conduct of network centric operations, the very cornerstone of U.S. military transformation.[59]

This challenge continues to be both technology and policy oriented. From the DoD's perspective, the continued funding of DoD level programs and research related to secure network access is imperative. The DoD must push for development of multiprotocol solutions, ad-hoc networking capabilities, and wireless access points capable of acquiring NSA certification for use with classified networks. From a commercial perspective, the majority of the technology advancements required involves improved wireless infrastructure worldwide. Wireless

consumers worldwide will continue to drive these improvements both in breadth and in throughput.

As this challenge involves deployment of ubiquitous wireless access points on classified networks, policy issues related to this merger must also be addressed. Because of today's limited authentication methods, information assurance policy and risk matrices do not allow for wireless access points on classified and critical networks.[60] The implementation of strong, enterprise-level auditing and authorization capabilities will allow these risk-driven policies to be mitigated. The required auditing and authorization identity management capabilities are detailed under challenges five and six respectively.

Tech Challenge #5: DoD Auditing and Administration Capabilities

President Obama's CNCI cybersecurity initiatives include developing and implementing a government-wide cyber counterintelligence (CI) plan necessary to coordinate activities across all Federal agencies to detect, deter, and mitigate the foreign-sponsored cyber intelligence threats to US and private information systems.[61] Any successful CI plan must include defenses against insider threats. Tech Challenge 5 involves creation of DoD-wide auditing and administration capabilities.

An enterprise-wide auditing capability is a critical component to identifying abnormal insider activity. It is a primary weapon against coercion and espionage. Currently, auditing is mandated and does take place during the certification and accreditation process as dictated by DoD Information Assurance Certification and Accreditation Process (DIACAP) and Federal Information Security Management Act (FISMA) Information Assurance controls.[62] Unfortunately, this auditing takes place at the local or system level, and this data is often only collected "to support technical analysis relating to misuse, penetration reconstruction, or other

investigations"[63] after an outage. This data would be far more useful in identifying trends and conspicuous insider actions if it were rolled up to a higher, centralized level in real-time.

In many cases, low and slow attacks go unnoticed as an internal threat vector navigates freely within the confines of our perimeter defenses. In some cases, such as Eligible Receiver, the attacks were planned government tests of our network security and vulnerability.

> Eligible Receiver is the code name of a 1997 internal exercise initiated by the Department of Defense. A "red team" of hackers from the NSA was organized to infiltrate the Pentagon systems. The red team was only allowed to use publicly available computer equipment and hacking software. Although many details about Eligible Receiver are still classified, it is known that the red team was able to infiltrate and take control of the Pacific command center computers, as well as power grids and 911 systems in nine major U.S. cities.[64]

In other more troubling instances such as Moonlight Maze and Titan Rain, the threat came from outside our borders.

> Moonlight Maze refers to a highly classified incident in which U.S. officials accidentally discovered a pattern of probing of computer systems at the Pentagon, NASA, Energy Department, private universities, and research labs that had begun in March 1998 and had been going on for nearly two years. …The invaders were systematically marauding through tens of thousands of files -- including maps of military installations, troop configurations and military hardware designs. The DoD traced the trail back to a mainframe computer in the former Soviet Union but the sponsor of the attacks is unknown and Russia denies any involvement. Moonlight Maze is still being actively investigated by U.S. intelligence. [65]

Titan Rain refers to a series of 2005 cyber assaults against U.S. computers traced back to 20 computer workstations in China's Guangdong province. "The precision of the attacks, the perfection of the methods and the 24-by-seven operations over two and a half years, and the number of workstations involved are simply not replicated in the amateur criminal community… Amateur cyber criminals do a lot of other things right, but this is an order of magnitude more disciplined than anything I have seen out of the hacker or amateur criminal community."[66]

The nature of these attacks and the amount of time it took for them to be discovered highlights the lack of internal monitoring and defense capabilities in cyberspace. These recently unclassified "cyber strikes against Western countries are more about spying and intelligence-gathering than about taking down systems and destroying information."[67] The DoD needs monitoring and auditing capabilities inside the perimeter defense systems to identify these low and slow intelligence gathering strikes.

Another component required to defend against these attacks is standardization and centralized administration of defense systems. The Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in January 2008 identified several initiatives to increase our cyber security posture.[68] The number one initiative was to "manage the Federal Enterprise Network as a single network enterprise."[69] Other initiatives focused on increasing measures to prevent and mitigate future attacks, the most pertinent to this discussion being the expansion of

> the EINSTEIN Program to all Federal departments and agencies. This will provide government officials with an early warning system to gain better situational awareness, earlier identification of malicious activity, and a more comprehensive network defense. The EINSTEIN Program helps identify unusual network traffic patterns and trends which signal unauthorized network traffic so security personnel are able to quickly identify and respond to potential threats.[70]

The second aspect of this technical challenge is the requirement for a DoD-wide centralized administration capability responsible for managing user authentication. Under the umbrella of authentication-centric tasks, this administrative toolset would allow personnel with appropriate credentials and role assignments to create new accounts, associate biometric templates with new users, modify user account information, and troubleshoot login issues. Further discussion on authentication capabilities can be found in the section discussing Tech Challenge 8.

This administrative toolset would also be used to manage authorization-centric tasks. The majority of authorization tasks are managed by the functional system administrators for a given system. These administrators are tasked with verifying need-to-know and need-to-access, assigning roles to user accounts, and troubleshooting data access issues. These administrative duties are delegated to the system level to ensure the access list is maintained by personnel who are most familiar with user data access requirements.

Another more centralized portion of the authorization administrative functions deals with macro-level access of end users. Each user account will be given access rights to different classification levels based on need-to-know, clearance, and job role. Further, users are assigned access authorizations to different application groupings based on job role. For example, the applications a Wing Commander requires are very different from those a logistics Senior Airman working on the flight line requires. These application groupings will be standardized and delivered in the form of virtual images (discussed in detail under Tech Challenge 7). In addition to these standardized virtual images, users will have access to a role- specific gallery of add-on applications that will be loaded by the end user much like iPhone applications are delivered today.

This challenge requires innovation on the part of commercial software providers to provide solutions scalable to the DoD enterprise for both administration and auditing. Of the four identity management facets, these two are the least mature in practice within the DoD and in development by commercial software providers. These aspects of identity management will take the longest amount of time to realize, but will provide the biggest benefit in terms of internal security and stability.

Tech Challenge #6: DoD Authorization Capability

Tech Challenge 6 requires the creation of a centralized role-based authorization system that leverages a directory of users to administer role-based access to data, applications, and devices. During a panel discussion on Identity Management, Role and Entitlement in August 2009, David Laurance of JPMorgan Chase highlighted seven common factors for applying roles to users in an enterprise[71] that are very analogous to those the military encounters daily. The following is a summary of the seven authorization aspects he discussed.

First, he highlighted the need to assign roles for authorization purposes.[72] Segmentation of roles allows an organization to control access to specific information based on need-to-know. Second, he highlighted the need to assign roles in order to identify expertise.[73] This separation of personnel by role allows an organization to assign access to information and systems based on community of interest membership or expertise.

Third, Mr. Laurance noted that roles allow an organization to separate access based on job assignments.[74] This role- based separation is useful in controlling access to job-centric applications such as those used on a CAOC floor or in a medical facility. Fourth, he explained that roles can be used to enforce polices and separate access based on duties such as system administration. Fifth, he discussed the value of abstracting identities from entitlements using roles to apply group membership[75] to individual identities. The group role is then assigned the entitlements for easier management purposes, thus eliminating the need to change privileges on each identity every time an access change is required.

Sixth, Mr. Laurance explained how roles can be used to speed automated provisioning[76] of identity access. Through the use of templates and groups, centralized identity management systems can provision new user accounts quicker and with less chance of missing specific access

requirements. Finally, he detailed how role authorization can be used for accountability purposes.[77] By segmenting rights and controlling access, it is much easier to discern who had access during fault resolution or during an investigation.

Aspects of the seven areas Mr. Laurance discussed above can be found throughout the DoD Global Information Grid. The DoD's Service-level portals and their associated data access architectures provide centralized access to myriad data repositories. The global address list initiatives fuse disparate lists of users into a common directory that could be a precursor to the required meta-directory for this tech challenge. The active directory consolidation efforts throughout the DoD address portions of the authorization and provisioning requirements discussed. However, most of these initiatives focus on establishment of user access, and the metrics they collect deal with user experience.

This challenge deals with consolidation and implementation of a complete solution that addresses all seven of the aspects raised earlier. At the same time, however, it is imperative that the DoD shift its focus toward addressing the growing issue of accumulation of access rights and discontinuing access and roles when they are no longer required to accomplish the mission. This issue will become more important as consolidation efforts eliminate the forced account recreation that happens when a user PCSs today. Eventually, a user will have a single access account that stays with him or her throughout a career. If authorization management controls are not put in place, users will continue to acquire access roles, but no revocation will take place. This is especially troubling in cases where a user may change jobs and retain elevated access to sensitive data. In order to begin managing authorization, the DoD requires a single repository or directory of users.

The deployment of the Defense Integrated Military Human Resources System (DIMHRS) offers the individual Services a departure point to begin this journey. The common core components of DIMHRS, shared across the Services, provide a standardized repository of all DoD users and a method of discerning when a given member's role may change. Although DIMHRS is no longer a unified DoD system, the shared core components (approximately 65% of the original requirements)[78] are still the best place to start an effort of this magnitude.

This challenge requires innovation on the part of commercial software providers to provide solutions scalable to the DoD enterprise. In order to be successful, the solution to this challenge must provide a single user repository including all role- specific security information. This repository must be responsive and must scale to a DoD-wide level. In order to be fault-tolerant, this solution should leverage the distributed processing power of the grid computing infrastructure provided by the solution to Tech Challenge 7.

Tech Challenge #7: Thin-Client/Image Management Solution

Tech Challenge 7 deals with creation of thin-client capabilities that are multi-classification capable. The backbone of the envisioned solution will leverage a series of regional processing centers that provide server farms to support thin-client delivery of content and applications to end users worldwide. These server farms will leverage grid computing technologies. According to Gartner, "[A] grid is a collection of resources owned by multiple organizations that is coordinated to allow them to solve a common problem."[79] Gartner further defines three commonly recognized forms of grid. The first is a computing grid, a grouping of multiple computers to solve one application problem.[80] The second is a data grid, multiple storage systems used to house one very large dataset or to provide disaster redundancy.[81] The

final form is the collaboration grid, multiple collaboration systems for collaborating on a common issue.[82]

Extending these grid concepts to 2035, it is envisioned that the DoD will have access to dispersed grid technology worldwide. This hybrid technology will leverage high- speed backbone Ethernet to present storage, collaboration, and computing resources virtually to military end users. Current estimates forecast that 100 Gbps Ethernet will be commercially available and widely adopted by 2016.[83] These virtual grids will leverage individually addressable memory, storage, and processors such that resources can be adjusted and targeted based on load and area of need.

These grids will provide a backbone for deployment of thin-client host servers that will provide end users with adjustable processing power in the field via the network. AF Research Labs[84] and USAFE have deployed secure image, virtualization, and thin-client pilot programs to prove the viability of these types of building block technologies.[85] The values of thin-client computing are centralization, disaster recovery, increased security, and streamlined management.

The centralization of computing resources in dispersed regional processing centers will allow the DoD to drastically cut military, civilian, and contracted administration personnel. This grid concept is the logical extension of the centralization and portal initiatives underway throughout DISA and the individual Services. By adding the distributed processing capabilities inherent in grid computing, the DoD satisfies the need for continuity of operations and disaster recovery. Grid computing provides recovery and redundancy at the most basic level. When connectivity is available and the grid is operating normally, the load is balanced across all available resources. If connectivity is interrupted for any reason, the grid compensates by migrating the load to the reduced set of available resources until connectivity can be restored.

Grid computing and thin-client architectures also provide increased security against malware and intrusions. Standardization of configurations and centralized administration reduce the risk of misconfiguration. Additionally, if NSA- certified encryption is used to secure data at rest and the processes running on the grid, the hosting of these resources can be commercially procured and hosted adding to the manpower savings highlighted earlier. Finally, grid computing and thin-client architectures streamline patch management. Server instances are patched as patches become available from source vendors.

The load is moved from the servers being patched to others waiting to be patched. The load is then transferred to the newly patched systems as they come back online. Users will receive the latest security patches without having to wait for them to be loaded. The addition of configuration management systems will allow administrators to load patches using batch scripts and scheduling software. The ability to create a scheduled job to patch all servers and virtual clients across the DoD without impacting end user access is a huge leap forward from the patch management and reporting environment we operate in today.

Based on the operational exploration and commercial maturity in this technology niche, the solution to this technical challenge should be deployable by 2020. This ten- year timeline is based on the required grid and virtualization technology maturation, the funding process within the US Government, and the Ethernet technology development still required to deploy a solution as envisioned above. Leveraging the current operational virtualization efforts and thin-client pilots as a starting point will save time, effort, and money. These efforts need to be aligned, integrated with an overall program timeline, and scaled to a DoD level.

Tech Challenge #8: DoD Authentication Capability

The eighth and final challenge deals with centralizing authentication services for the DoD. DoD Common Access Card (CAC) initiatives, Air Force directory integration efforts, and Defense Knowledge Online portal consolidation programs led by DoD/NII are examples of efforts addressing portions of this authentication service. The CAC is a precursor to the wearable biometric device discussed under Tech Challenge 1.

One of President Obama's CNCI cybersecurity initiatives is to increase the security of our classified networks.[86] To that end, efforts should be made to expand the CAC program to add certificates for access to classified data networks to include Top Secret. Policy is needed to create a certificate authority infrastructure on classified networks across the DoD. Additionally, the CAC program roadmap should be overlaid on the timeline associated with Tech Challenge 1 with the eventual replacement of the CAC by biometric devices. The addition of biometric validation schemes will enhance the authentication infrastructure.

Authentication efforts such as active directory consolidation will need to be rolled up to a DoD level. Elimination of Service, MAJCOM, and system-level "county options" is critical to overcoming the issues associated with disparate identities across the DoD infostructure. Currently, end users acquire credentials for each network, major systems, and each Service portal. Single-sign-on efforts offer a stopgap by associating CAC credentials to a unique identity for a given portal or functional system. The better method is to consolidate the core user identity associated with the CAC and the directories used for validation. By eliminating the extraneous foreign identity contexts, the need for associations, meta-directories, and single sign-on applications are eliminated.

Policy barriers and loss of control by current administrators and owners are the largest barriers to this challenge. Nevertheless, of all of the challenges discussed thus far, this capability is the most mature today. This challenge is the foundation for the other seven challenges required to arrive at the envisioned solution. Work done in satisfying this challenge will continue all the way through Tech Challenge 1, as challenge one and eight are both authorization- centric capabilities. Tech Challenge 8 should be completed by 2018 given the work ongoing across the Services today.

Solution Caveats

One of President Obama's CNCI cybersecurity initiatives is to coordinate and redirect research and development (R&D) efforts in order to develop strategies and structures for coordinating all cyber R&D sponsored or conducted by the US government.[87] The eight technology challenges described in the preceding sections and the associated solution envisioned are not set in stone. Any of the technical challenges can be adopted by the DoD in an effort to secure the DoD cyber infostructure. The solution and challenges presented have not been evaluated for feasibility under current budgetary restrictions, nor have cost savings been computed to present Return on Investment figures. The assumption is that this paper will be used to generate discussion about identity management efforts and consolidation programs, and that those discussions will generate action plans that include cost benefit analyses.

Many of the challenges are based on programs that currently exist within the DoD or on technologies available today. Given these facts, one might expect the timeline for implementation of the overall solution to be much closer than 2035. The 2035 timeline is based on current and past capability development trends. Of particular note is how little network security methodologies and tools have changed since inception in the 1990s.

Further, the joint nature of the envisioned solution and the budgetary issues to be overcome will add considerable overhead and time to these efforts. In fact, the programmatics, policy changes, resourcing, and planning will most likely take longer than the commercial development of the required technologies. Every effort has been made to choose technologies that complement each other and that require limited R&D efforts. In most areas where R&D is required, the majority of the funding and development is projected to be driven by consumer need. The only exception is the RFID biometric device. It is not anticipated that civilian users will find this sort of device necessary or, for that matter, palatable given privacy concerns.

Chapter 5: Summary and Conclusions

According to the US National Intelligence Council in its Global Trends 2025 report:

> Even in the military realm, where the US will continue to possess considerable advantages in 2025, advances by others in science and technology, expanded adoption of irregular warfare tactics by both state and nonstate actors… and growing use of cyber warfare attacks increasingly will constrict US freedom of action.[88]

The military's use of cyberspace as a warfighting domain in current operations is vulnerable to hackers and malware. Today's perimeter defense cyber strategy is antiquated and operates on the tenet of trust. Attackers currently use this inherent trust against us once they breach our perimeter defenses. As attacks become more sophisticated and organized, the US military's freedom of operation in the cyber domain will become increasingly constrained. By 2035, the emerging threats posed by insiders, artificial intelligence and nation-states such as China will require game-changing innovations to defend cyberspace.

This paper's findings are that the Air Force and DoD should research, promote, and fund solutions to the eight major challenges required to deploy the proposed solution. This solution will mitigate emerging threats to the DoD's freedom of action in cyberspace by 2035. By

eliminating the DoD's reliance on military networks, security and agility are increased. Security is increased by centralizing and standardizing administration and management, and by reducing the capability of cyber attackers to target military operators. This is done by leveraging commercial carriers and secure wireless networks for access. The military operator becomes obscured and fades into the background noise provided by billions of civilian users on the Internet.

Cyber agility is increased by creating an environment that allows users to access mission-essential information regardless of where that information resides. The use of grid computing further bolsters agility by providing disaster recovering, load balancing, and continuity of operations as a byproduct of design and deployment. Grid computing combined with NSA-approved encryption will also allow the DoD to divest itself from the care and feeding associated with server farm ownership.

These eight challenges, when combined with anticipated changes in the cyberspace environment between now and 2035, provide a foundation for a fundamental shift in how the AF and DoD as a whole approaches cyber security and access to information. Utilizing backcasting techniques, my research has shown how shifts in policy and technology procurement in eight challenge areas can lead to a solution by 2035.

Appendix A: Figures

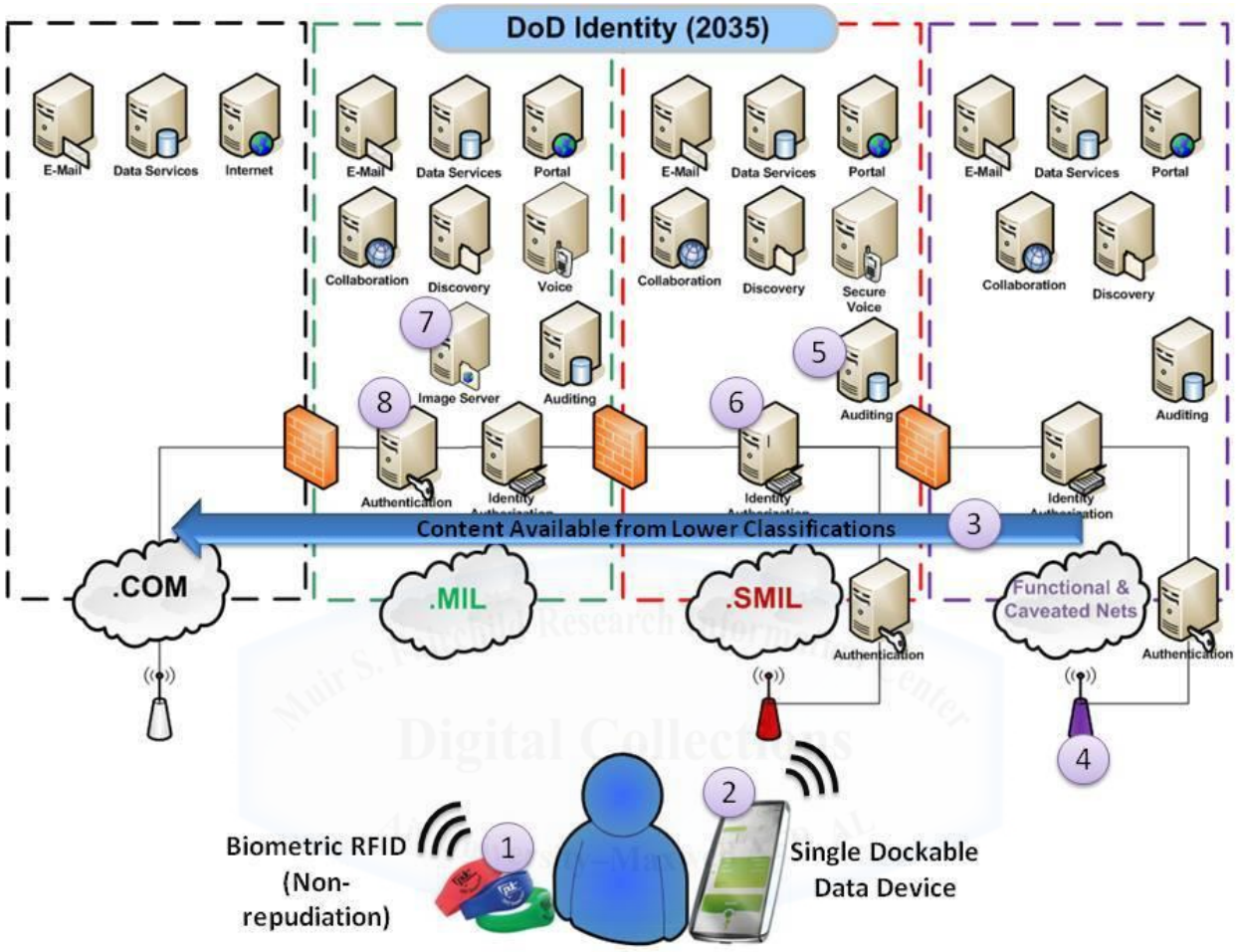

Figure 1: Proposed Solution and Associated Challenges

Figure 2: Precision Dynamics Corporation's Smart Rewearable Wristband[89]

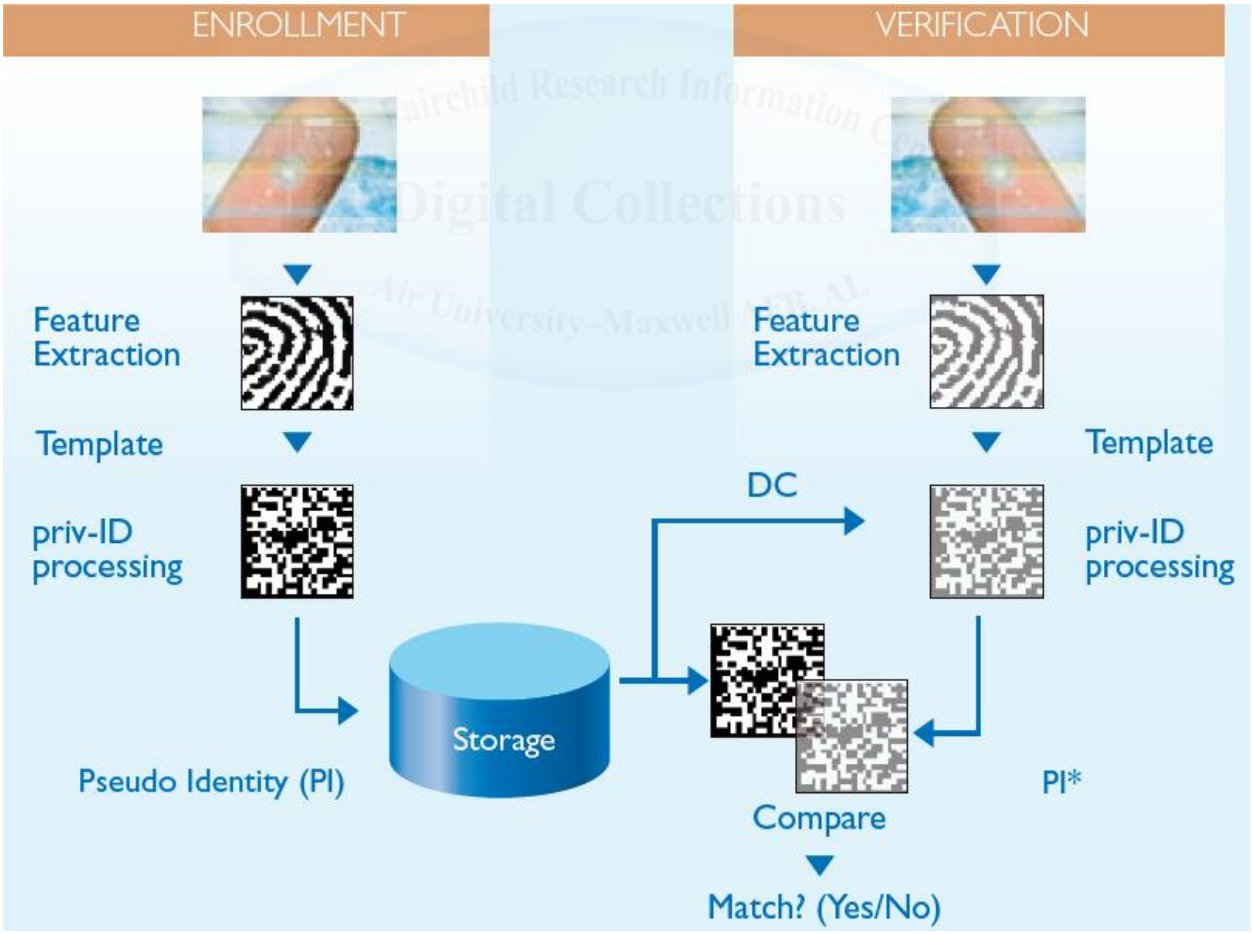

Figure 3: Private Identity Biometric Processing[90]

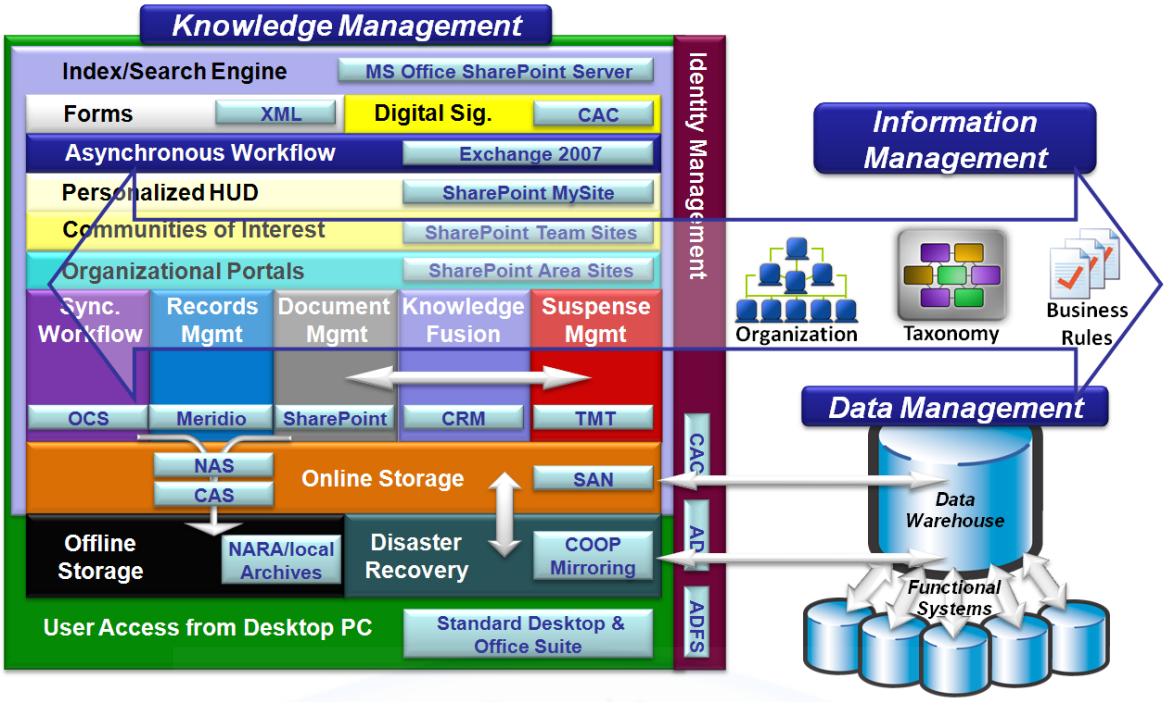

Figure 4: MNF-I KM Service-Oriented Architecture End State[91]

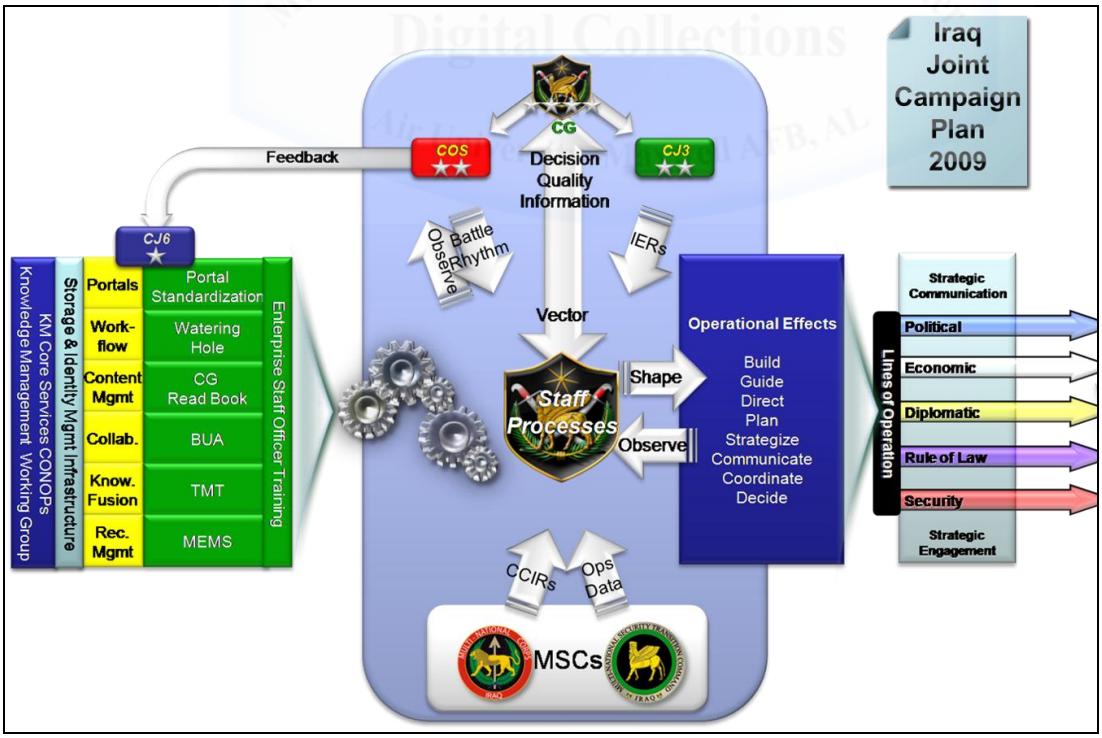

Figure 5: MNF-I Knowledge Management Support to Lines of Operation[92]

Endnotes

[1] England, *The Definition of "Cyberspace"*, 1.
[2] Ibid.
[3] Rumsfeld, *Information Operations Roadmap* (Redacted), 44-45.
[4] Lt Gen Robert Elder as quoted in Peter A. Bauxbaum, "Air Force explores the Next Frontier," *GCN Magazine*, Feb 19, 2007.
[5] JP 6-0, *Joint Communications System*, IV-5.
[6] Paliotta, *Beyond the Maginot-Line Mentality*, 22.
[7] DISA, Internet-NIPRNET DoD DMZ Engineering Plan, 6.
[8] Grant, Rebecca. "Battling the Phantom Menace," Air Force Magazine, 40.
[9] Maj Gen Hawkins, Ronnie, Deputy Director DISA, Speech to AF Mission Critical Symposium, Slide 20, 27 Mar 2008.
[10] Ibid.
[11] Fox, *Information Assurance and the Defense in Depth*, 58.
[12] Witty, et al., *Identity and Access Management Defined*, 3.
[13] Ibid.
[14] Grant, Rebecca. "Battling the Phantom Menace," Air Force Magazine, 40.
[15] Ibid.
[16] Ibid.
[17] Witty, et al., *Identity and Access Management Defined*, 3.
[18] Grant, Rebecca. "Battling the Phantom Menace," Air Force Magazine, 42.
[19] Ibid.
[20] General Hobbins, Tom, COMUSAFE. Speech at Battlespace Information 2007 Conference in Brussels, Belgium.
[21] Ibid.
[22] Ibid.
[23] Mazanec, *The Art of (Cyber) War*, 1.
[24] National Intelligence Council, *Global Trends 2025: A Transformed World,* 71.
[25] Wagner, Countering Cyber Attacks, *The Futurist*, 16.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* 8.
[30] Thornburgh, et al., The Invasion of the Chinese Cyberspies, 1.
[31] Ibid.
[32] Cetron, *World War 3.0: Ten Critical Trends for Cybersecurity,* 49.
[33] Naraine, Cybercrime, More Widespread, Skillful, and Dangerous than Ever
[34] Larus, Spending Moore's Dividend, 64.
[35] A. Bhargav-Spantzel, et al, *Privacy preserving multi-factor authentication with biometrics*, 550.
[36] The White House, "The Comprehensive National Cybersecurity Initiative", http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] Precision Dynamics Corporation, PDC Smart Rewearable Wristband Product Sheet, 1.
[41] Mordini and Massari, "Body, Biometrics and Identity", 489.
[42] Ibid.

[43] Mostrous and Brown, "Microsoft seeks patent for office 'spy' software", 1.
[44] Priv-ID. Technology Primer on Private Identity Matching, 2.
[45] Department of Homeland Security, Western Hemisphere Travel Initiative.
[46] van der Ploeg, I, *The Machine-Readable Body. Essays on Biometrics and the Informatization of the Body*.
[47] Woodward, *Army Biometric Applications, Identifying and Addressing Sociocultural Concerns.*23.
[48] Apple, iPad Product Specifications, http://www.apple.com/iPad.
[49] General Dynamics, Sectera Edge Smart Phone, http://www.gdc4s.com/documents/GD-Sectera_Edge-w.pdf.
[50] General Dynamics, TVE Desktop, http://www.gdc4s.com/documents/GD-TVE-w2.pdf.
[51] Ibid.
[52]Joint Staff, Joint Warrior Interoperability Demonstration 2004 Final Report, 1.
[53] MNF-I, MNF-I Knowledge Management CONOPS, 1.
[54] Campbell, Unleashing Semantic Web's Power, 15-16.
[55] General Hobbins, Tom, COMUSAFE. Speech at Battlespace Information 2007 Conference in Brussels, Belgium.
[56] Touré, Hamadoun. Economist, "Finishing the Job," 18.
[57] Ibid.
[58] Ibid.
[59] DoD, Joint Transformation Roadmap, 73.
[60] DoD Information Assurance Certification and Accreditation Handbook, 112.
[61] The White House, "The Comprehensive National Cybersecurity Initiative", http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[62] DoDi 8500.2, Information Assurance (IA) Implementation. Section 5.7.9.3. http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf, 7.
[63] Ibid.
[64] Frontline, Cyber War!, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar /warnings/.
[65] Frontline, Cyber War!, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar.
[66] Greenmeier, Larry. Scientific American. http://www.scientificamerican.com/article.cfm?id=chinas-cyber-attacks-sign
[67] Ibid.
[68] Department of Homeland Security, "Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks", http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm
[69] The White House, "The Comprehensive National Cybersecurity Initiative", http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[70] Department of Homeland Security, "Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks", http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm
[71] Kampman, Kevin, "Role" World Challenges, http://identityblog.burtongroup.com/bgidps/role_management
[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Miller, Jason, Federal News Radio. DoD decides one-size does not fit all with DIHMRS. http://www.federalnewsradio.com/index.php?nid=35&sid=1668301
[79] Gartner, What Grid Computing is Really About. http://www.gartner.com/DisplayDocument?id=490645
[80] Ibid.
[81] Ibid.
[82] Ibid.
[83] CIR, The Path to 100 Gbps Networks, Section 5.2

[84] Hughes, Interview with AFRL/ATSPI Chief during Blue Horizons's site visit, October 2009.
[85] USAFE/A6 Strategic Plan, 12 December 2008, 3.
[86] The White House, "The Comprehensive National Cybersecurity Initiative", http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[87] Ibid.
[88] National Intelligence Council, *Global Trends 2025: A Transformed World,* xi.
[89] Precision Dynamics Corporation, PDC Smart Rewearable Wristband Product Sheet, 1.
[90] Priv-ID. Technology Primer on Private Identity Matching, 2.
[91] MNF-I, MNF-I Knowledge Management CONOPS, 18.
[92] MNF-I CJ6, Briefing to Microsoft Air Force Symposium 2009, Slide 30.

Bibliography

Apple. iPad Product Specifications. http://www.apple.com/ipad/, Accessed 23 March 2010.

Bhargav-Spantzel et al. Privacy preserving multi-factor authentication with biometrics, *Journal of Computer Security*; Jan 2007, Vol. 15 Issue: Number 5, p529-560.

Blair, Dennis C., Director of National Intelligence. Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. 2 Feb 2010.

Campbell, Ted. Unleashing Semantic Web's Power, *Insights*, 4Q, 2005, p12-23.

Centron, Marvin J. and Owens, Davies. "World War 3.0: Ten Critical Trends for Cybersecurity." In *The Futurist*, 46-52. Sep-Oct 2009.

CIR, The Path to 100 Gbps Networks, 17 January 2008.

Department of Homeland Security, "Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks", http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm, Accessed 15 February 2010.

Department of Homeland Security, Western Hemisphere Travel Initiative, http://www.getyouhome.gov/html/eng_map.html, Accessed 22 December 2009.

DISA, Internet-NIPRNET DoD DMZ Engineering Plan, 8 February, 2008.

DoD Information Assurance Certification and Accreditation (DIACAP) Handbook. Version 1.0, 15 July 2008.

DoD, Joint Transformation Roadmap, 24 January 2004.

DoDi 8500.2, Information Assurance (IA) Implementation. Section 5.7.9.3.
http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf, Accessed 12 March 2010.

Elder, Robert, Lt General, USAF as quoted in Peter A. Bauxbaum, "Air Force explores the Next Fronter," *GCN Magazine*, 19 Feb 2007.

England, Gordon, Deputy Secretary of Defense. Memorandum, subject: *The Definition of "Cyberspace"*, 12 May 2008.

Fox, Jonathan M., MAJ, USA. Information Assurance and the Defense in Depth: A Study of INFOSEC Warriors and INFOSEC Cowboys, Kansas, 2003.

Frontline, Cyber Warfare!, Directed by: Kirk, Michael. Original airdate: 24 April 2003. Web excerpts: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar, Accessed 12 March 2010.

Gartner Research, What Grid Computing is Really About. http://www.gartner.com/DisplayDocument?id=490645, Accessed 15 February 2010.

General Dynamics, Sectéra Edge Smartphone Product Specifications, http://www.gdc4s.com/documents/GD-Sectera_Edge-w.pdf, Accessed 23 March 2010.

General Dynamics, TVE Desktop Product Specifications, http://www.gdc4s.com/documents/GD-TVE-w2.pdf, Accessed 23 March 2010.

Grant, Rebecca. "Battling the Phantom Menace," Air Force Magazine, p38-42. April 2010.

Greenmeier, Larry. "China's Cyber Attacks Signal New Battlefield Is Online", Scientific American, 17 September, 2007. http://www.scientificamerican.com/article.cfm?id=chinas-cyber-attacks-sign, Accessed 15 February 2010.

Hawkins, Ronnie D Jr., Maj Gen, DISA Deputy Director, Briefing to AF Mission Critical Symposium, Slide 20, 27 Mar 2008.

Hobbins, Tom, General, USAF. COMUSAFE. Speech at Battlespace Information 2007 Conference in Brussels, Belgium.

Hughes, Jeff A. AFRL/ATSPI Chief. Briefing and interview during Blue Horizon's site visit, Oct 2009.

JP 6-0, *Joint Communication System*, Washington D.C., 2006.

Joint Staff, Joint Warrior Interoperability Demonstration 2004 Final Report, http://www.cwid.js.mil/public/cwid05fr/htmlfiles/u110sei.html. 2004, Accessed 23 Mar 2010.

Kampman, Kevin, "Role" World Challenges, 11 August 2009. Excerpts from panel discussion on Identity Management, Role and Entitlement at the Catalyst Conference. http://identityblog.burtongroup.com/bgidps/role_management, Accessed 28 March 2010.

Krekel, Bryan. Northrop Grumman Corporation. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* Oct 2009.

Larus, James. Spending Moore's Dividend, *Communications of the ACM*, May 2009, Vol. 52 Issue 5, p62-69.

Libicki, Martin C. RAND Corporation. *Cyberdeterrence and Cyberwar.* October 2009.

Mazanec, Brian M. "The Art of (Cyber) War." In *The Journal of International Security Affairs*, Spring 2009-Number 16.

Miller, Jason, Federal News Radio. DoD decides one-size does not fit all with DIHMRS. http://www.federalnewsradio.com/index.php?nid=35&sid=1668301, Accessed 15 February 2010.

Mordini, Emilio and Massari, Sonia, "Body, Biometrics and Identity", In *Bioethics*, Volume 22, Number 9 2008, p488-498.

Mostrous, Alexi and Brown, David, "Microsoft seeks patent for office 'spy' software", In *The Times*, http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193480.ece, Accessed 10 Feb 2010.

Multi National Force-Iraq CJ6, MNF-I Knowledge Management Concept of Operations, 1 October 2008.

Multi National Force-Iraq CJ6, Briefing on Knowledge Management Efforts to Microsoft Air Force Symposium, April 6, 2009.

Naraine, Ryan. Cybercrime More Widespread, Skillful, and Dangerous than Ever, 13 Apr 2006. Downloaded from http://www.foxnews.com/story/0,2933,191375,00.html

National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008.

Paliotta, Allan R., Beyond the Maginot-Line Mentality: A Total-Process View of Information Security Risk Management, *Information Systems Security.* 2001.

Precision Dynamics Corporation, PDC Smart Rewearable Wristband Product Sheet, http://www.pdcorp.com/downloads/PDC Smart Rewearable Flyer.pdf, Accessed 15 Feb 2010.

Priv-ID, *Technology Primer on Private Identity Matching: "Biometrics 2.0*", http://www.priv-id.com/images/Technology-primer.pdf, Accessed 16 January 2010.

Rumsfeld, Donald H., Secretary of Defense. *Information Operations Roadmap*, (Redacted), 44-45. 30 Oct 2003.

The Singularity Institute for Artificial Intelligence. *What is the Singularity?* http://www.singinst.org/overview/whatisthesingularity. 27 Oct 2009.

Thornburgh, Nathan, et al., The Invasion of the Chinese Cyberspies, *Time South Pacific,* Issue 35, 5 Sep 2005.

USAFE/A6 Strategic Plan, 12 Dec 2008.

van der Ploeg, I, The Machine-Readable Body. *Essays on Biometrics and the Informatization of the Body*. 2005.

Wagner, Cynthia G., Countering Cyber Threats, *The Futurist*, 16. May-June 2007.

The White House. "The Comprehensive National Cybersecurity Initiative." http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative, Accessed 15 February 2010.

Touré, Hamadoun. Finishing the Job, *Economist,* Vol. 392, Issue 8650. p18.

Witty, Roberta J., et al. Gartner Corporation. *Identity and Access Management Defined.* Nov 2003.

Woodward et al, RAND Corporation. *Army Biometric Applications, Identifying and Addressing Sociocultural Concerns,* 2001.